Lê Ngọc Kiều Anh

MSSV: 22520047

**BÀI TẬP AN TOÀN MẠNG MÁY TÍNH BUỔI 9**

**Câu 1. Mô tả các kỹ thuật cơ bản của virus máy tính**

Các kỹ thuật cơ bản:

1. **Kỹ thuật lây nhiễm**

- Là kỹ thuật cơ bản cần phải có của mỗi virus, có thể đơn giản hoặc phức tạp tuỳ loại virus.

+ Kỹ thuật lây nhiễm Boot Record / Master Boot của đĩa: thay thế BR hoặc MB trên phân vùng hoạt động với chương trình virus.

+ Kỹ thuật lây nhiễm file thi hành: chương trình virus sẽ được ghép vào file chủ bằng cách nối thêm, chèn giữa, điền vào khoảng trống, ghi đè.

+ Thuật toán để lây nhiễm một file .COM.

1. **Kỹ thuật định vị trên vùng nhớ**

- Phân phối một vùng nhớ để thường trú, chuyển toàn bộ chương trình virus tới vùng nhớ này, sau đó chuyển quyền điều khiển cho đoạn mã tại vùng nhớ mới với địa chỉ segment:offset mới.

- Là một kỹ thuật quan trọng đối với các chương trình virus dạng mã máy (virus Boot, virus file). Virus macro và virus Script thực chất là các lệnh của chương trình ứng dụng nên không cần tiến hành kỹ thuật này.

1. **Kỹ thuật kiểm tra sự tồn tại**

- Mỗi virus chỉ nên lây nhiễm/kiểm soát một lần để đảm bảo không làm ảnh hưởng đến tốc độ làm việc của máy tính.

- Virus phải kiểm tra sự tồn tại của chính mình trước khi lây nhiễm hoặc thường trú:

+ Kiểm tra trên đối tượng bị lây nhiễm

+ Kiểm tra trên bộ nhớ

- Kỹ thuật kiểm tra thường là:

+ Dò tìm đoạn mã nhận diện trên file hoặc bộ nhớ.

+ Kiểm tra theo kích thước hoặc nhãn thời gian của file.

1. **Kỹ thuật thường trú**

- Các virus boot phải phân phối một vùng nhớ riêng để lưu giữ chương trình virus bao gồm mã lệnh, biến, vùng đệm.

- Các virus file cần phải kiểm tra xem chương trình đã thường trú chưa, nếu

chưa sẽ định rõ vùng nhớ muốn sử dụng, copy phần virus vào bộ nhớ, sau đó khôi phục file chủ và trả quyền điều khiển về cho file chủ.

1. **Kỹ thuật mã hoá**

- Nhằm che giấu mã lệnh thực sự của chương trình virus.

- Thủ tục mã hoá cũng chính là thủ tục giải mã

1. **Kỹ thuật nguỵ trang**

- Nhằm giấu giếm, nguỵ trang sự tồn tại của virus trên đối tượng chủ.

- Những virus sử dụng kỹ thuật này thường chậm bị phát hiện nên có khả năng lây lan mạnh.

1. **Kỹ thuật phá hoại**

- Đa dạng

- Phá hoại dữ liệu trên máy tính

- Phá hỏng một phần máy tính

1. **Kỹ thuật chống bẫy**

Chọn lọc file trước khi lây nhiễm theo một số tiêu chí nào đó nhằm tránh những file bẫy của chương trình Antivirus.

+ Không lây nhiễm các file có số trong tên file

+ Không lây nhiễm những chương trình sử dụng nhiều mã lệnh đặc biệt.

+ Không lây nhiễm các file có tên liên tục (ví dụ

aaaaa.com…).

+ Không lây nhiễm các file liên tục có cùng kích thước.

+ Không lây nhiễm các file ở thư mục gốc.

+ Không lây nhiễm các file có lệnh nhảy và lệnh gọi zero.

**9. Kỹ thuật tối ưu**

Các kỹ thuật viết mã và thiết kế nhằm tối ưu chương trình về tốc độ và kích thước.

**Câu 3. Tìm và nêu đặc điểm 2-3 loại mã độc (virus, worm,…) xuất hiện trong thời gian gần đây (tên, nguồn gốc, đặc điểm, phương thức phá hoại, biện pháp phòng chống, nguồn tham khảo).**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tên** | **Nguồn gốc** | **Đặc điểm** | **Phương thức phá hoại** | **Biện pháp phòng chống** | **Nguồn tham khảo** |
| Sogu (Virus) | Một nhóm hacker có liên kết với Trung Quốc, 2023 | Sogu là một virus gián điệp lây qua USB, đặc biệt nhắm đến các ngành dược phẩm, công nghệ và năng lượng. Mã độc này tìm kiếm các tài liệu nhạy cảm và sao chép chúng vào thư mục mã hóa, từ đó gửi về máy chủ của kẻ tấn công. | Sogu tự động kích hoạt và thiết lập sự hiện diện lâu dài trên hệ thống bằng cách tạo khóa registry, thêm tác vụ vào Windows Task Scheduler để mã độc tiếp tục hoạt động mỗi khi hệ thống khởi động lại. | Hạn chế sử dụng USB từ nguồn không rõ ràng, sử dụng các phần mềm bảo mật để phát hiện hành vi xâm nhập, và thường xuyên quét hệ thống để phát hiện các dấu hiệu của mã độc. | **[Sogu Virus](https://www.bleepingcomputer.com/news/security/usb-drive-malware-attacks-spiking-again-in-first-half-o)** |
| Snowydrive (Backdoor Worm) | Nhóm hacker UNC4698 | Là một dạng mã độc backdoor worm, Snowydrive lây nhiễm qua USB và thiết lập cổng sau cho phép kẻ tấn công kiểm soát hệ thống từ xa. | Khi nạn nhân kích hoạt tệp thực thi từ USB, mã độc thiết lập backdoor và thực hiện các thao tác hệ thống như sao chép, chỉnh sửa registry, mở tệp tin, thậm chí cung cấp truy cập từ xa. | Hạn chế sử dụng các ổ USB từ nguồn không rõ ràng, sử dụng phần mềm bảo mật có khả năng phát hiện mã độc USB, và kiểm tra các hoạt động nền trên hệ thống để ngăn chặn các mối đe dọa trước khi chúng lây lan. |  |